NCUA LETTER TO CREDIT UNIONS

NATIONAL CREDIT UNION ADMINISTRATION
1775 Duke Street, Alexandria, VA 22314

DATE: June 2011 **LETTER NO.: 11-CU-09**

TO: Federally Insured Credit Unions

SUBJ: Online Member Authentication Guidance
Compliance Required by January 2012

ENCL: FFIEC Supplement to Authentication in an Internet Banking Environment

Dear Board of Directors:

As more credit union members are conducting transactions online, NCUA and other federal financial regulators are issuing updated guidance to address Internet threats which have changed significantly over the past several years. Sophisticated hacking techniques and growing organized cyber criminal groups are increasingly targeting financial institutions, compromising authentication mechanisms and security controls, and engaging in online account takeovers and fraudulent electronic funds transfers.

Enclosed is a supplement to authentication guidance that was last issued in 2005 by the Federal Financial Institutions Examination Council.[1] The supplement reinforces the risk management framework specified in the 2005 guidance, *Authentication in an Internet Banking Environment*. More importantly, the supplement updates supervisory expectations for effective member authentication mechanisms, layered security and other controls to combat growing identity theft attacks and online transaction frauds.

Federally insured credit unions will be expected to adapt appropriate strategies from the supplement to strengthen and enhance controls by January 2012. Beginning in 2012, at credit unions offering electronic services, NCUA examiners will evaluate these controls under the enhanced expectations outlined in the supplement.

The rest of this letter highlights key precautions that federally insured credit unions should take if offering electronic services:

- Review and update risk assessments whenever a new electronic financial service is implemented or modified and when conditions warrant (e.g. changes in threats, etc.). To enhance online identity verification and reduce identity theft risk, perform periodic risk assessments to evaluate the effectiveness of existing member authentication controls in response to the threats. Adjust your level of authentication controls accordingly.

[1] Federal Financial Institutions Examination Council member agencies include Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, Office of Thrift Supervision, and the State Liaison Committee.

- Do not rely exclusively on access controls provided by authentication controls. It is essential to implement appropriate layered security at the transaction process level based on your service operations and threat environment to facilitate fraud detection and respond to suspicious activity. Layered security means that a vulnerable control installed at a different point can be compensated for by the strength of other control layers. The layered security approach will significantly strengthen the overall security of your Internet-based services. Increasing evidence has shown that layered security can effectively thwart and reduce money transfer fraud. Review the effective layered controls specified in the layered security program under the supplement.

- If engaging in high-risk Internet-based transactions -- such as utilizing automated payment mechanisms (e.g. wire transfers and ACH payments) or offering commercial banking services -- employ a combination of controls that cover both initial account access and subsequent transaction processing in order to effectively mitigate identity theft and prevent online transaction frauds.

- Educate members to be aware of the protection provided (and not provided) relative to electronic fund transfers under Regulation E. Advise members that your credit union may ask members to:

    - Provide electronic banking credentials;
    - Implement alternative risk control mechanisms suggested by your credit union; and
    - Contact authorities when they become aware of suspicious account activity.

    In addition, commercial members may be required to perform their own risk assessments and controls evaluations.

All of these actions should be taken to protect credit unions as well as members from cyber fraud. These precautions are intended to prevent the damage that fraud can due to your reputation and finances.

Sincerely,

/s/

Debbie Matz
Chairman

Enclosure